to: Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

from: Daniel E. Geer, Jr., Sc.D.
Principal, Geer Risk Services, LLC
P.O. Box 390244
Cambridge, Mass. 02139
Telephone: +1 617 492 6814
Facsimile: +1 617 491 6464
Email: dan@geer.org

date: 23 Apr 2007

re: Hearing, Wednesday 25 April 07, entitled
Addressing the Nation’s Cybersecurity Challenges:
Reducing Vulnerabilities Requires Strategic Investment
and Immediate Action

Introduction

The Nation's cybersecurity challenges are profound and not easily addressed. Perfection is not possible; rather this is entirely a matter of risk management, not risk avoidance. Easy to say. Hard, though not impossible, to do. Starting yesterday would be good. Money alone will not solve anything. Policy alone will not solve anything. Fixing what isn't broken will waste money capital and policy capital; fixing what is broken will require both. Wishful thinking, whether explicit or implicit, intentional or delusional, will allow the problem to get bigger.

In the testimony which follows, I make no attempt to argue from first principles or to provide every supporting footnote that would be required to prove the assertions made; I don't think you want it and the page limit prevents it. I do, however, have all the proof that can be had, and stake my professional reputation on what is said here. I trust that you have invited me because you are aware of that reputation and my bona fides in these matters. The material is brief in the hope that brevity increases the likelihood it will be read. This is not your last chance to get my attention; I hope it is not my last chance to get yours.

Priority number one: A system of security metrics.

"You cannot manage what you cannot measure" is a cliche´, but, happily, one of the great scientists of all time, William Thompson, Lord Kelvin, put it as well as it can be put:

> When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science.

As we stand here today, we have some security metrics. None of them are perfected though many are good enough for decision making if, and only if, they are collected by persons whose aim is truth rather than positioning. In late 2003, the Computing Research Association and the National Science Foundation held an invitation-only workshop to determine the ten-year "grand challenges" for NSF investment in cybersecurity. Of the four grand challenges settled upon, one speaks directly to this: Within a decade, we must have a body of quantitative information risk management as sophisticated as the then existing body of financial risk management. That item was mine, and I had the honor of presenting it to this body immediately after the conclusion of the workshop.

Good metrics are not cooked in the kitchen. They are not created simply because the Congress demands them. Like statistics, they can mislead. In your line of work, you doubtless know this better than I and I know it well. The purpose of risk management is to improve the future, not to explain the past. Security metrics are the servants of risk management, and risk management is about making decisions under uncertainty. Therefore, the only security metrics we are interested in are those that support decision making about risk for the purpose of managing that risk. I urge the Congress to put explaining the past, particularly for the purpose of assigning blame, behind itself. Demanding report cards, legislating under the influence of adrenaline, imagining that cybersecurity is an end rather than merely a means — all these and more inevitably prolong a world in which we are procedurally correct but factually stupid. A clearinghouse review of what we know how to measure and how good what we know is at predicting the future would be a good start as we do not even know what it is that we do not know.

Priority number two: The demand for security expertise outstrips the supply.

Information security is perhaps the hardest technical field on the planet. Nothing is stable, surprise is constant, and all defenders work at a permanent, structural disadvantage compared to the attackers. Because the demands for expertise so outstrip the supply, the fraction of all practitioners who are charlatans is rising. Because the demands of expertise are so difficult, the training deficit is critical. We do not have the time to create, as if from scratch, all the skills required. We must steal them from other fields where parallel challenges exist. The reason cybersecurity is not worse is that a substantial majority of top security practitioners bring other skills into the field; in my own case, I am a biostatistician by training. Civil engineers, public health practitioners, actuaries, aircraft designers, lawyers, and on and on — they all have expertise we can use, and until we have a training regime sufficient to supply the unmet demand for security expertise we should be both grateful for the renaissance quality of the information security field and we should mine those other disciplines for everything we can steal. If you can help bring people into the field, especially from conversion, then please do so. In the meantime, do not believe all that you hear from so-called experts. Santayana had it right when he said that "Scepticism is the chastity of the intellect; it is shameful to give it up too soon, or to the first comer."

Priority number three: What you cannot see is more important than what you can.

The opposition is professional. It is no longer joyriders or braggarts. Because of the sheer complexity of modern, distributed, interdigitated, networked computer systems, the number of hiding places for unwanted software and unwanted visitors is very large. The complexity, for the most part, comes from competitive pressure to add feature-richness to products; there is no market-leading product where one or a small group of people knows it in its entirety, and components from any pervasive system tend to be used and re-used in ways that even their designers did not anticipate. Were there no attackers, this would be a miracle of efficiency and goodness. But unlike any other industrial product, information systems are at risk not from accident, not from cosmic radiation, and not from clumsy operation but from sentient opponents. The risk is not, as some would blithely say, "evolving" if by evolving the speaker means to invoke the course of Nature. The risk is due to intelligent design, and there is nothing random about it.

Because complex systems fail complexly, it is not possible to anticipate all the failure modes of large and therefore complex information systems. This complexity provides both opportunity and hiding places for attackers. Damping out complexity is not something that even the Congress can take on, but security failures come from it as surely as dawn comes from the east. Given that most software license agreements are an outrage, it is high time that security failures in software systems be deemed *per se* offenses. Just as my ignorance of the law is no defense and my swimming pool is an attractive nuisance whether I like it or not, ignorance of installed vulnerabilities can no longer be a defense for any party.

Priority number four: Information sharing that matters.

On the Internet every sociopath is your next door neighbor; you can never retreat to a safe neighborhood. Your ability to defend depends on your ability to know what the current threat profile is, both generally to all and specifically to yourself. For any given attack, you have zero ability to know whether you are a target of choice or a target of opportunity unless you share attack data with others.

Our Centers for Disease Control lead the world, full stop. There are only three things that make this so: (1) Mandatory reporting of communicable disease, (2) Longitudinal analysis and the skill to separate statistical anomalies from genuine harbingers of important change, and (3) Away teams to handle outbreaks of, say, Ebola. All the rest is details. Of the three, the one that matters most is the mandatory reporting of communicable disease, and explicitly on the grounds that individual medical privacy must yield when the public risk is above threshold.

No General Counsel will share information risk data willingly, and no Chief Information Security Officer outranks his/her GC. Shared information does always carry some acute chance that it contains a previously unknown embarrassment, while any benefit from sharing is diffuse and delayed. Any person is risk averse when they don't know what risk they are taking and more so when the risk is involuntary; the GC is rational to not share data, in other words. The Congress should be wary of legislating irrationality, as always.

To get information shared the need is for a technical guarantee of harmlessness rather than a procedural guarantee. This is, in other words, a straight-up research question: How to provide technical de-identification of useful cybersecurity data so that that data can be shared with low or no risk to its source. Such technical protection should be open-sourced so that its strength can be independently evaluated *a´ priori* rather than the "trust us" nature of a procedural guarantee. Fund this research.

Priority number five: Accountability, not access control.

Information is the coin of the economic realm, and information that is used is information that moves about. Winners have the most information in play; losers have too much. Security technology is the fine line between the most information in play and too much information in play. The conventional answer to protecting information is to in some way limit who can do what and to which. Authentication (who you are) and Authorization (what you can do, given who you are) represent the conventional approach, sometimes jointly called Access Control. The problem is, these technologies do not scale and if you try to have ever finer control over the avalanche of new data items appearing by the second, you will be contributing to the complexity that is the bane of security.

What does scale is Accountability. In a free country, you don't have to ask permission for much of anything, but that freedom is buttressed by the certain knowledge that if you sufficiently screw things then up you will have to pay. The economics of the access-control model of information security do not scale; rather economics favor an accountability model focused on the monitoring of information use rather than the gatekeeping of information access. This means surveillance of data use in the sense of being able to reconstruct how information is used when it is used badly. This does not mean to throw away our existing investment in access control, but further investment in that will only produce inefficiency and a false sense of security.

We are, sadly if necessarily, making surveillance a commonplace of physical security; it is no longer possible to live in a world without cameras. We will have to, sadly if necessarily, make surveillance a commonplace of cybersecurity. As you consider how to make these dreadful choices, I suggest that the unit of observation be a datum, not a person, that if a surveillance system has to protect the digital world, that that surveillance be directed at data, not persons. If anything, this is risk management applied to risk management.

Summary

- We need a system of security metrics, and it is a research grade problem.
- The demand for security expertise outstrips the supply, and it is a training problem and a recruitment problem.
- What you cannot see is more important than what you can, and so the Congress must never mistake the absence of evidence for the evidence of absence, especially when it comes to information security.
- Information sharing that matters does not and will not happen without research into technical guarantees of non-traceability.
- Accountability is the idea whose time has come, but it has a terrible beauty.